Automatic Intrusion detection system

1st Siddharth Bhorge
Electronic And Telecommunication
Vishwakarma institute of Technology
Pune, Indian
siddharth.bhorge@vit.edu

2nd Swapnil Patil
Electronic And Telecommunication
Vishwakarma institute of Technology
Pune, Indian
swapnil.patil21@vit.edu

3rd Devyani Ushir
Electronic And Telecommunication
Vishwakarma institute of Technology
Pune, Indian
devyani.ushir21@vit.edu

4th Saburi Waghmare
Electronic And Telecommunication
Vishwakarma institute of Technology
Pune, Indian
saburi.waghmare21@vit.edu

5th Sakshi Bhosale
Electronic And Telecommunication
Vishwakarma institute of Technology
Pune, Indian
sakshi.bhosale19@vit.edu

***Abstract*—This paper presents a novel approach to developing a Smart Intruder Detection System using OpenCV, Python, and a mobile phone. The system provides robust surveillance and prompt notification in case of unauthorized access to a premises. By leveraging advanced image processing techniques, including motion detection and object recognition, potential intrusions can be accurately identified. The system integrates with a mobile phone using the IP Webcam application, enabling remote monitoring. Immediate notification is facilitated through the Twilio API, sending text messages upon intrusion detection. By combining OpenCV, Python, IP Webcam, and Twilio, a cost-effective and efficient Smart Intruder Detection System is realized, addressing the growing demand for enhanced home security. The proposed solution offers flexibility, convenience, and widespread compatibility with popular software tools and technologies.**

Keywords— Intrusion, Ip Webcam, TwilioAPI, detection.

I. INTRODUCTION

The increasing demand for effective home security systems, there is a growing need for innovative solutions that provide robust surveillance and timely notification in the event of unauthorized access to premises. This paper introduces a novel approach to developing a Smart Intruder Detection System using computer vision, Python programming, and mobile phone integration. The proposed system leverages the power of computer vision to analyze real-time video feeds and accurately identify potential intrusions. By implementing advanced image processing techniques, such as motion detection and object recognition, the system can efficiently detect and alert homeowners about security breaches.

To enhance convenience and accessibility, the system integrates with mobile phones, transforming them into dedicated surveillance cameras. This integration is achieved using a mobile application, which allows users to remotely monitor their premises using their existing mobile devices. To ensure prompt and reliable notifications, the system utilizes an API service that enables the sending of text messages to designated recipients. This feature enables homeowners to take immediate action upon intrusion detection, further strengthening the security of their premises. By combining the capabilities of computer vision, Python programming, mobile phone integration, and reliable notification services, a cost-effective and efficient Smart Intruder Detection System can be developed. This approach addresses the increasing demand for enhanced home security while utilizing popular software tools and technologies, offering a practical solution for homeowners seeking reliable surveillance and prompt notification capabilities.

II. LITERATURE SURVEY

Nasrin Sultana et al. reviews recent works and discusses continued difficulties in applying ML/DL to NIDS. This study described several intrusion detection algorithms utilizing ML/DL approaches and explored the newly emerging topic of Software-Defined Networking. (Due to the effectiveness of deep learning in assessing network security, many factors must be taken into account when deploying NIDS. It's difficult to develop a feature selection technique for classifiers. Real-time intrusion detection in high-speed networks is a potential future route to create a centralized SDN controller. This survey may aid in R&D personnel's comprehension of creation in SDN environment employing DL method. [1]

Neha Bhadwal et al. finds In order to uphold peace and guarantee the protection of a nation's citizens, border monitoring is a crucial responsibility in national defense and security. The border security personnel currently perform this monitoring manually, which requires a significant amount of resources and men. Designing an automated border surveillance device that may carry out the surveillance characteristic without requiring human intervention is necessary. Such systems can save money and lessen the risk to human life by setting up central control rooms away from the border region. Due to safety concerns, complete automation of border surveillance is still not possible. By utilizing cutting-edge technology, the smart border monitoring system may assist improve the security of border areas while saving labor and resources. Additionally, it can aid in more effective and precise control of undesirable and suspicious activity. [2]

Richard Lin et al Due to the difficulties that current IDSs face from arbitrary intrusion categories and processing capacity, this study suggests a taxonomy to describe contemporary IDSs. Due to the growing network traffic and security threat, the study of intrusion detection systems has drawn a lot of interest. It's crucial to choose the ways carefully because each strategy has advantages and disadvantages. Heuristic-based methods offer the advantage of requiring no prior understanding of threats, but because of their high computing cost, they struggle in real-time applications. The authors provide a taxonomy to outline contemporary, tables and figures to make it simple to understand the big picture, as well as two well-known open source tools for analyzing in order to provide a thorough understanding of IDSs and application needs.. [3]

Shadi et al. creates a new hybrid model based on the best aspects of the network transaction data that may be utilized to calculate the intrusion scope threshold degree. According to the experimental findings, the hybrid approach appreciably reduced the computational and time complexity had to calculate the feature association impact scale. The ability to produce both high and low false negative rates is problematic, though. The hybrid method has enhanced accuracy, a high false negative rate, a low false positive rule, Random Tree, REPTree, AdaBoostM1, Decision Stump, and Nave Bayes. The suggested hybrid model decreases the accuracy rate and detection time using the NSL-KDD dataset, which has been used to evaluate and simulate IDS performance. [4]

Amitabh Mishra et al. researches that Intrusion detection has become increasingly important in network security, especially in wireless ad hoc networks, which are vulnerable to attacks. Intrusion IDSs keep track of audit data, search for intrusions, and launch the appropriate response. The work that has been done on intrusion detection in cell ad hoc networks is surveyed in this article. Detecting and responding to intrusions in wireless ad hoc networks requires resource-constrained methods that analyze vast amounts of trace data or attack fingerprints. Anomaly-detection-based systems are more practical since they don't require extensive changes to routing protocols and enable local trace analysis and anomaly detection in each node. [5]

Daniel C. Nash, & Thomas L develops An intrusion detection system uses a linear regression model to estimate power consumption and identify potential battery exhaustion attacks. The proposed IDS was effective in determining while the gadget has used greater strength than is important to maintain a assured battery life. method strength estimation may be utilized as a primary line of defense, and system-call delays had been used to lessen the impact of programs that were idea to be aberrant. whether or not an based on self-contained strength size may be utilized to detect breaches unrelated to batteries is an unresolved subject. [6]

Sheyangi Pan et al. develops a hybrid IDS that learns temporal state-based specifications for power system scenarios in an organized and automated manner. The implementation and validation of an prototype allowed it to categorize disruptions, regular manipulate operations, and cyber-assaults with accuracy. The commonplace pathways mining-primarily based utilizes a fusion of synchro phasor information and facts from relay, community protection logs, and EMS logs to permit tasteful tracking of an electric transmission distance safety machine. it's miles better suitable for the massive quantity of data found in electricity structures and became taught the use of a popular direction mining approach. Updating to do actual-time classification from cutting-edge machine inputs and integrating the classifier with an clever adaptive control framework would require further development. [7]

Zakira Inayat et al. presents SMD can access cloud resources thanks to mobile cloud computing, but since connection links are iffy, security is a major concern. The cloud-based IDRS is discussed in this article in relation and cloud resources, along with any unresolved problems and potential fixes. Due to their communication relationship and multi-tenancy functionality, security is a contentious topic for SMDs and MCC. [8]

Deris Stiawan et al. The evaluation of our system has revealed how to avoid expectation. Analyze, analyze, and discover difficult issues to develop intrusion prevention. Future study will concentrate on signature accuracy with behavior-based prevention, an experiment with our real traffic network data set. The correctness of the signature, traffic volume, topology design, quota usage logging, protection of intrusion prevention systems, sensor monitoring, and UTM collaboration are only a few of the problems with PS. To avoid anticipation, IPS combines firewall technology with Intrusion Detection System. [9]

Vinayakum Ar et al. examines the effectiveness of diverse machine getting to know algorithms on wonderful datasets of malware which can be publicly available. in an effort to create a bendy and effective IDS to perceive and categorize unplanned and unpredictable cyber-attacks, deep neural networks are being investigated. To behavior the benchmark, the DNN model is applied to additional datasets including NSL-KDD, UNSW-. It has been demonstrated through extensive experimental testing outperform traditional machine learning classifiers. In order to handle and examine large amounts of facts in actual time, this look at indicates a hybrid intrusion detection alert machine the usage of a dispensed deep gaining knowledge of model. The proposed structure is the primary machine which can collect community-level and host-degree pastime in a disbursed way the usage of to more efficiently stumble on attacks, outperforming traditional machine learning classifiers. [10]

Bharat Manvi et al focuses on the key components of person detection. We can tell if someone is acting improperly by watching the movement of key body parts. For the first frame, a bounding box is selected. Therefore, we'll show you a novel technique for finding a discrepancy in a surveillance footage in this part. Today, surveillance consists solely of recording videos to a disk drive. The best choice isn't yet these. The criminal history demonstrates that the offenses were reported formally. This project was completed using methods that are on par with cutting-edge methods utilized in computer vision.. gives optimum performance over a range of 1 to 10 meters as well. The system's performance, however, starts to significantly degrade as the distance approaches 20 m. [11]

Majed Al-Asiri et.al research covered intrusion detection using physical measurements. An introduction of systems and a taxonomy of IDSs were developed to meet the special features of systems, particularly the consideration of physical metrics in contrast to application metrics. Lastly, a benchmark dataset was used in an experiment. created in a lab and made publicly available to test the efficiency of physical measures in intrusion detection. It is clear from the results that detection methods that are based solely on network traffic outperform those that combine physical measures, associated application parameters, and network metrics. [12]

Aswin Wibisurya et al. suggested is a system that can keep an eye on and manipulate the door remotely, provide you with a warning if movement is detected close to the door, give relied on people get right of entry to control the door, view

the door get right of entry to history log and user access, alert you if the door remains open after the allotted amount of time, and sound the alarm should the door remain open. be forcedly opened. According to the simulation results, the system can accurately identify a movement at a distance of 1.6 meters ahead when the sensor is positioned at a height of 48.5 cm with the direction pointing down, but the detection will be less accurate at a distance greater than 1.6 meters. The simulation findings also demonstrate that signals transmitted between a smartphone and a door lock are correctly secured by SSL so that they cannot be intercepted by hackers. [13]

K. Mukundini et al develops IoT networks need to be protected from attacks because they are very susceptible to them, so solutions must be developed and put to the test. For this project, platform was created and used as a proving ground for comprehending and executing IoT attacks on the network. In order to employ machine learning techniques to identify network risks, data were collected from the implemented network. Four machine learning algorithms were used to classify the data as normal and modified hazardous attack data. methods were tried. [14]

Sharath pankanti et al researches Closed-circuit television cameras have proliferated in popularity in recent years. the use of computer-imaginative and prescient algorithms to mine and decipher video facts, which include motion, challenge identities, and event instances, is currently on the rise in video processing systems. CCTV monitoring is typically associated with nuclear power plants or covert military activities, but inexpensive cameras are enabling a variety of applications that place cameras on objects, in structures, and in public places. [15]

III. METHODOLOGY

From below Fig 1 it is shown that firstly, the IP Webcam application is installed and configured on the mobile phone. this allows the phone to function as a surveillance camera, streaming video feeds over the network. To establish communication between the mobile phone and the computer, both devices need to be connected to the same network. This ensures that the computer can access the video stream by utilizing the IP address generated by the IP Webcam. Once the connection is established, the computer utilizes the OpenCV library for real-time analysis of the video stream. Advanced image processing techniques, including motion detection and object recognition, are implemented to accurately identify potential intrusions within the video feed.

To provide immediate notification, the system integrates with the Twilio API. When an intrusion is detected, the system sends text messages to a designated recipient, alerting them of the intrusion. Additionally, after a person leaves the room, a notification is triggered after a 7-second delay to avoid false alarms. Furthermore, the system saves recorded activity in a designated folder, allowing users to review the events captured when a person enters and leaves a room. The text message notifications also include date and time information, providing a comprehensive record of the intruder's entry and exit times.

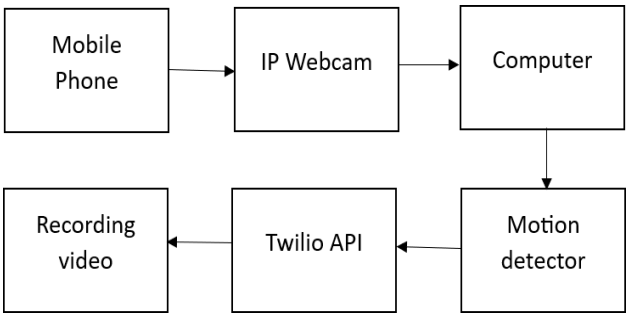

Fig.1. (*Block diagram of ID system)*

A. Flow chart For check person is present or noe

The function is_person_present is designed to determine whether a person is present in a given frame. It takes a frame as input, along with an optional threshold parameter. Within the function, the variable foog is declared as global, indicating its reference from an outer scope. To identify the presence of a person, the function applies background subtraction to the frame using foog.apply(frame), resulting in the creation of a mask called fgmask. This mask is then further processed to eliminate shadows by thresholding, where values above 250 are set to 255 (white) and the rest are set to 0 (black). The refined mask undergoes morphological operations, such as dilation, to enhance its quality. Next, the function detects contours in the refined mask using cv2.findContours. If contours exist and the area of the largest contour is above the provided threshold, the function proceeds to draw a bounding rectangle around the detected person and adds a text label indicating "Person Detected" on the frame. It then returns True along with the modified frame. Below Figure 2 shows a visual representation of the flowchart explaining the process of determining if a person is present or not.

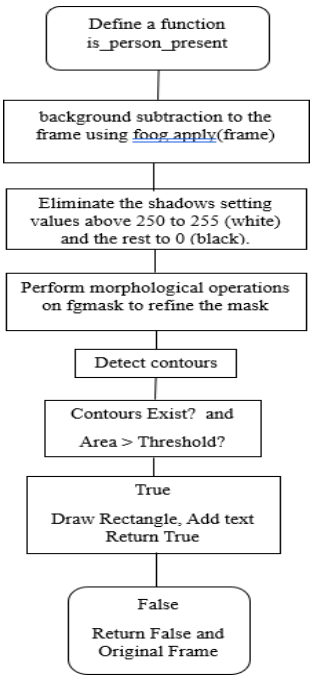

Fig.2. (*Flow diagram for person is present or not)*

B. *Algorithm for reading video from phone's Camera*

Algorithm 1 describes the process of reading frames from a phone's camera using OpenCV. The algorithm begins by setting the window mode to normal, allowing for resizing of the window. It initializes variables for calculating the frames per second (FPS) and a frame counter. The starting time is noted using the time. time() function. Next, a video capture object is created, specifying the URL of the camera stream. The algorithm enters a while loop to continuously read frames from the video stream. Within the loop, it reads a frame using cap.read(). If the frame is not successfully read (indicated by ret being false), the loop breaks.For each successfully read frame, the frame counter is incremented by 1. The average FPS is calculated by dividing the frame counter by the elapsed time since the start. The FPS value is then displayed on the frame using cv2.putText(). The frame is shown on the screen using cv2.imshow().The algorithm checks for the 'q' key press using cv2.waitKey(1). If 'q' is pressed, the loop is exited. Once the while loop is finished, the video capture object is released and the window is destroyed, freeing up system resources.

Algorithm 1 Reading from your phone's Camera

Require: Setting Window mode to normal so it can be resized

1: Initialize variables for calculating FPS and frame_counter
2: Note starting time using time. Time()
3: Open video capture object using specified URL
4: **while** read frames from the video stream
   I. Read frame from video stream using cap.read()
   II. Frame was not successfully read ret it false break
   III. Increment frame counter by 1.
   IV. Calculate average FPS by dividing frame counter
   V. Display FPS on frame using CV2.putText()
   VI. Show the frame
   VII. If q is pressed waitkey(1)
5: **end while**
6: Release video capture object and destroy window
7: **end**

Fig.3. (*Algorithm for Reading video from phone's camera)*

C. *Flow chart for Final Application*

The code analyzes video frames to detect the presence of a person. It starts by initializing variables and reading frames from a video source. Background subtraction is applied to separate background from foreground elements. The resulting foreground mask is refined through thresholding and morphological operations. Contours are then detected in the mask, and their areas are checked against a threshold to determine if a person is present. If a person is detected, a bounding box is drawn around them, and a label is added to indicate the detection. The code keeps track of consecutive detections to ensure reliability. Once a sufficient number of detections occur, the program confirms the presence of a person and records the entry time. It periodically checks if the person disappears, using a patience timer to avoid false positives. If the person remains undetected beyond the patience time, the program sets the status to indicate their absence, records the exit time, and saves the annotated frames. Various information, such as the current time, room occupancy status, and patience time, is displayed on the frame. The code calculates the frames per second (FPS) and displays the annotated frame. The user can quit the program by pressing the 'q' key, and the video source is released when all frames are processed.

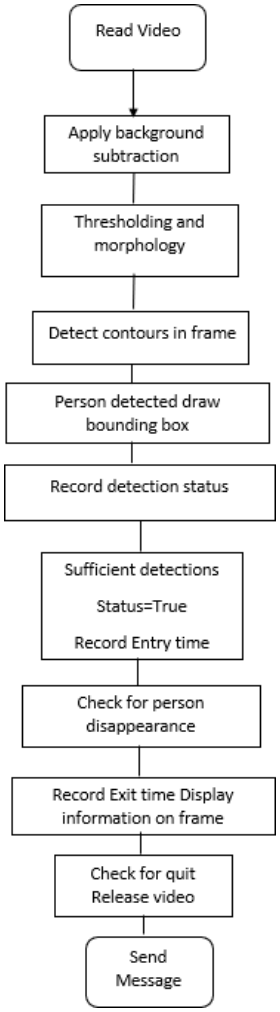

Fig.4. (*Flow chart for final application of ID system)*

D. *Algorithm for sending Message*

The algorithm is designed to send an alert message using Twilio. It begins by extracting the required information, such as the Twilio account SID and authentication token, recipient's phone number, and Twilio trial number, from the info_dict data structure. These details are stored in the variables account_sid, auth_token, recipient_number, and trial_number, respectively. With the necessary information at hand, the algorithm proceeds to create a new client object using the Twilio account SID and authentication token. This client object acts as a connection to the Twilio API, enabling communication with the messaging service. To compose the message body, the algorithm formulates the content of the

alert message. This can include relevant information such as a notification or warning about a specific event or situation.

Next, the algorithm utilizes the client object to send the alert message. It calls the create method on the client object, passing the recipient's phone number (to), the Twilio trial number (from_), and the message body (body) as parameters. This triggers the sending of the message through the Twilio platform.The create method returns a message object that represents the sent message. This object can be further utilized for tracking and handling the status of the message if desired. The algorithm retrieves the necessary Twilio credentials and recipient information, creates a client object, composes the alert message, and sends it using Twilio's create method.

Algorithm 2 Sending Alert Message Using Twilio

Require: info_dict (contains Twilio account SID, authentication token, recipient's number, and trial number)

1: Retrieve Account SID and authentication token from info_dict & assign to account_sid and auth_token
2: Create a new client object using account_sid and auth_token
3: Compose the body of the message to be sent and assign it to the variable body
4: Retrieve the recipient's no & twilio trial no from info_dict
5: Use the client object to create a new message by calling create method with following parameters:
   I. To: recipient number
   II. From: twilio_number
   III. Body: Body
6: To create method will send the message and return a message Object representing the sent message
7: **end**

Fig.5. (*Algorithm of sending message)*

IV. RESULT AND ANALYSIS

In the context of the project's results and analysis, it was observed that by connecting an IP webcam to a computer, a live stream of video could be established. This functionality was depicted in Figure 6, where the video feed was successfully displayed. Furthermore, Figure 7 demonstrated the system's capability to detect a person within the video stream. The person was accurately identified and labeled accordingly. Additionally, the system automatically initiated recording upon detecting the presence of a person.

To showcase the recording process, Figure 8 illustrated the saving of the video after the person exited the frame. Specifically, seven seconds after the person left the frame, the recording ceased and was saved in a designated folder. This seamless recording and saving mechanism ensured that relevant footage was captured efficiently. Moreover, the project incorporated the Twilio API to enable the receipt of notifications. As demonstrated in Figure 9, a message was successfully received via the Twilio API, containing essential information regarding the person's entry and exit times. This feature enhanced the system's functionality by providing real-time updates on individuals entering the frame.

Fig.6. (*live stream video of ID system)*

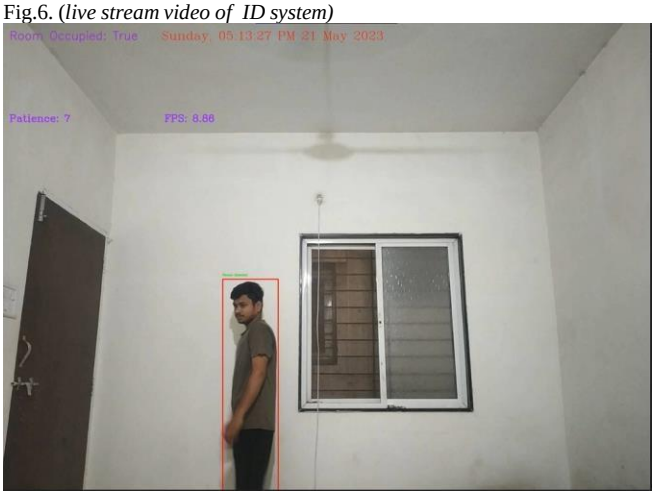

Fig.7. (*Result for Person is detected)*

Fig.8. (*Video saved in file)*

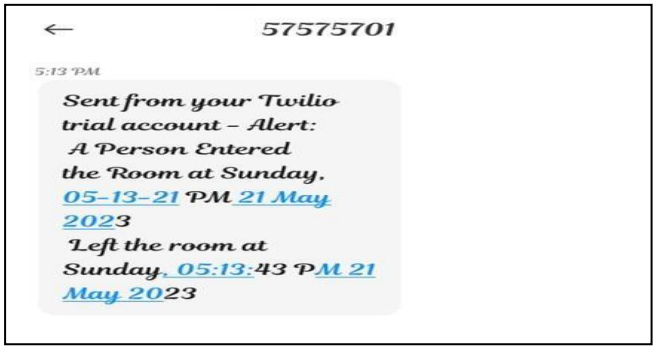

Fig.9. (*Alert message received using Twilio API)*

V. CONCLUSION AND FUTURE SCOPE

The Smart Intruder Detection System, developed using OpenCV, Python, and a mobile phone, offers an innovative solution for enhancing home security. By utilizing computer vision techniques like motion detection and object recognition, the system accurately identifies potential intrusions in real-time as shown in Fig 1. Integration with the Twilio API enables homeowners to receive immediate text message notifications upon intrusion detection (Fig 5), allowing them to take prompt action. The IP Webcam application facilitates convenient mobile phone integration and remote monitoring.

To improve the system, potential avenues include researching advanced algorithms for more accurate intrusion detection, incorporating multi-camera support for comprehensive surveillance coverage, integrating with other security systems, developing a dedicated mobile application for an enhanced user experience, and leveraging cloud-based storage and analysis for scalability. Additionally, configuring the IP Camera with a static IP address would eliminate the need for frequent address changes, and making the system globally accessible would remove the limitation of relying on the same network/WIFI connection.

REFERENCES

[1] Sultana, N., Chilamkurti, N., Peng, W., & Alhadad, R. (2019). Survey on SDN based network intrusion detection system using machine learning approaches. *Peer-to-Peer Networking and Applications*, *12*, 493-501.

[2] Bhadwal, N., Madaan, V., Agrawal, P., Shukla, A., & Kakran, A. Smart border surveillance system using wireless sensor network and computer vision. In *2019 international conference on Automation, Computational and Technology Management* (pp. 183-190). IEEE.

[3] Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, *36*(1), 16-24.

[4] Aljawarneh, S., Aldwairi, M., & Yassein, M. B. (2018). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *Journal of Computational Science*, *25*, 152-160.

[5] Mishra, A., Nadkarni, K., & Patcha, A. (2004). Intrusion detection in wireless ad hoc networks. *IEEE wireless communications*, *11*(1), 48-60.

[6] Nash, D. C., Martin, T. L., Ha, D. S., & Hsiao, M. S. (2005, March). Towards an intrusion detection system for battery exhaustion attacks on mobile computing devices. In *Third IEEE international conference on pervasive computing and communications workshops* (pp. 141-145). IEEE.

[7] Pan, S., Morris, T., & Adhikari, U. (2015). Developing a hybrid intrusion detection system using data mining for power systems. *IEEE Transactions on Smart Grid*, *6*(6), 3104-3113.

[8] Inayat, Z., Gani, A., Anuar, N. B., Anwar, S., & Khan, M. K. (2017). Cloud-based intrusion detection and response system: open research issues, and solutions. *Arabian Journal for Science and Engineering*, *42*, 399-423.

[9] Stiawan, D., Abdullah, A. H., & Idris, M. Y. (2010, June). The trends of intrusion prevention system network. In *2010 2nd International Conference on Education Technology and Computer* (Vol. 4, pp. V4-217). IEEE.

[10] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *Ieee Access*, *7*, 41525-41550.

[11] Thyagarajmurthy, A., Ninad, M. G., Rakesh, B. G., Niranjan, S., & Manvi, B. (2019). Anomaly detection in surveillance video using pose estimation. In *Emerging Research in Electronics, Computer Science and Technology: Proceedings of International Conference, ICERECT 2018* (pp. 753-766). Springer Singapore.

[12] Al-Asiri, M., & El-Alfy, E. S. M. (2020). On using physical based intrusion detection in SCADA systems. *Procedia Computer Science*, *170*, 34-42.

[13] Aldawira, C. R., Putra, H. W., Hanafiah, N., Surjarwo, S., & Wibisurya, A. (2019). Door security system for home monitoring based on ESp32. *Procedia Computer Science*, *157*, 673-682.

[14] Kiran, K. S., Devisetty, R. K., Kalyan, N. P., Mukundini, K., & Karthi, R. (2020). Building a intrusion detection system for IoT environment using machine learning techniques. *Procedia Computer Science*, *171*, 2372-2379.

[15] Senior, A., Pankanti, S., Hampapur, A., Brown, L., Tian, Y. L., Ekin, A., & Lu, M. (2005). Enabling video privacy through computer vision. *IEEE Security & Privacy*, *3*(3), 50-57.